

RESEARCH OUTPUTS / RÉSULTATS DE RECHERCHE

Fichiers d'assurances et respect des libertés

Poullet, Yves

Published in:
Bulletin des Assurances

Publication date:
1984

Document Version
le PDF de l'éditeur

[Link to publication](#)

Citation for pulished version (HARVARD):

Poullet, Y 1984, 'Fichiers d'assurances et respect des libertés', *Bulletin des Assurances*, Numéro 271, p. 573-615.

General rights

Copyright and moral rights for the publications made accessible in the public portal are retained by the authors and/or other copyright owners and it is a condition of accessing publications that users recognise and abide by the legal requirements associated with these rights.

- Users may download and print one copy of any publication from the public portal for the purpose of private study or research.
- You may not further distribute the material or use it for any profit-making activity or commercial gain
- You may freely distribute the URL identifying the publication in the public portal ?

Take down policy

If you believe that this document breaches copyright please contact us providing details, and we will remove access to the work immediately and investigate your claim.

C.R.I.B. — Centre Docum.	
Date Entrée	N° Inv.
06 MAI 1987	248
Cote de	
Ran	

*Pour le Centre
et son
secrétaire
Yves*

FICHIERS D'ASSURANCES ET RESPECT DES LIBERTES

YVES POULLET

Directeur du Centre de Recherches Informatique et Droit de Namur
Chargé de cours à la Faculté de Droit de Namur

1. Une récente étude menée par le National Computer Center (N.C.C.) de Manchester (1), analysant l'impact des réglementations de protection des données sur les secteurs industriels, gros consommateurs d'informations spécifiques, rangeait au second rang de ces secteurs, le monde de l'Assurance.

Nul ne contestera le besoin particulièrement important des assurances d'obtenir une information riche et de haute qualité. Elle est le fondement même de l'appréciation du risque, objet de la couverture proposée par l'assureur (1 bis). L'article 9 de la loi du 11 juin 1874 (2) consacre implicitement ce droit de l'assureur à l'information quant au risque assuré.

2. Le caractère sensible des informations ainsi récoltées, leur nombre et la possibilité de leur dissémination rapide font craindre qu'au-delà de l'atteinte à notre « vie privée », plus fondamentalement ne soient remises en cause certaines de nos libertés (3),

(1) N.C.C., The Impact of International Data Protection Regulations on special Information - intensive Sectors of Industry, Final Report, 2 volumes, in Data Security and Confidentiality. A joint research programme between ADI, GMD and N.C.C. sponsored by the Commission of the European Communities and National Governments, Janvier 1984.

(1 bis) Sur ces observations, lire également l'annexe 12 du 2^e rapport d'activité de la CNIL (1^{er} octobre 1980 - 15 octobre 1981), La documentation française, 233 et s.

(2) Article 9: « Toute réticence, toute fausse déclaration de la part de l'assuré, même sans mauvaise foi, rendent l'assurance nulle lorsqu'elles diminuent l'opinion du risque ou en changeant le sujet de telle sorte que l'assureur, s'il en avait eu connaissance, n'aurait pas contracté aux mêmes conditions ». Comp. l'article L 113-2 du Code français des Assurances.

(3) Sur la nécessité d'élargir le débat et de ne pas se préoccuper de la seule vie privée mais des libertés individuelles et publiques en général, nos réflexions in « L'informatique menace-t-elle nos libertés », « La télématique, Aspects techniques, juridiques et socio-politiques », Actes du colloque de Namur des 5 et 6 décembre 1983, Story-Scientia, 1984. On notera à ce propos le titre de la loi française du 6 janvier 1978 relative « à l'informatique, aux fichiers et aux libertés ».

ainsi celle d'obtenir un crédit, celle de se déplacer en automobile, etc. et que ces traitements ne soient l'occasion de discriminations (3 bis) entre les fichés.

Diverses réglementations tant au niveau national, qu'international prétendent conjurer ce « péril » (4). Chez nous, l'actuel ministre de la Justice a déposé le 10 novembre 1983 sur le bureau de la Chambre des Représentants, un projet de loi relatif à la protection de certains aspects de la vie privée. Ce projet fera incessamment l'objet des discussions de la Commission de la justice.

3. Notre propos n'est pas de proposer une réflexion critique du projet actuel (5). Nous chercherons simplement à décrire le plus concrètement possible les implications du projet sur l'informatisation des entreprises d'assurances. A titre non seulement comparatif mais également de suggestion, nous évoquerons certaines solutions de la pratique née de diverses réglementations

(3 bis) On parle de discrimination lorsque la différence de traitements entre deux personnes manque d'une base objective c'est-à-dire de pertinence. Sur l'intérêt de consacrer la notion de discrimination à côté de celle de vie privée, nos réflexions in Banques de données, Entreprises et Vie privée, Actes du colloque de Namur, Bruxelles, CREA-DIF, 1980, p. 201.

(4) Dispositions sur le plan international:

- O.C.D.E.: lignes directrices régissant la protection de la vie privée et les flux transfrontières de données de caractère personnel, 23 septembre 1980;
- Conseil de l'Europe: Convention pour la protection des personnes à l'égard du traitement des données à caractère personnel, 21 janvier 1981.

Législations sur le plan national (en Europe):

- Autriche: Datenschutzgesetz (D.S.G.), 18 octobre 1978;
- Hongrie: loi du 27 janvier 1981;
- Danemark: lois danoises, n° 293 sur les registres privés, n° 294 sur les registres publics, 8 juin 1978;
- France: loi n° 78-17 du 6 janvier 1978, informatique, fichiers et libertés;
- Luxembourg: loi du 31 mars 1979 réglementant l'utilisation des données nominatives dans les traitements informatiques;
- Norvège, loi du 9 juin 1978 sur les registres de personnes;
- République fédérale d'Allemagne: Bundesdatenschutzgesetz, 27 janvier 1977;
- Suède: Data act. 11 mai 1973 (amendé le 1^{er} juillet 1979);
- Pays-Bas: Tijdelijke wet aanmelding geautomatiseerde persoonsregistraties, 9 juillet 1982;
- Islande: loi du 25 mai 1981 sur la collecte systématique de données personnelles;
- Suisse: Richtlinien für die Bearbeitung von Personendaten in der Bundesverwaltung, 16 mars 1981.

(5) A propos de cette critique, J. Berleur -Y. Pouillet, Le droit à la vie privée selon le projet Gol, J.T., 1982, 769 et s. Pour une présentation du projet, J.P. Spreutels, Vie privée et Informatique - La recherche d'un équilibre, Conférence donnée le 11 octobre 1983, CIEAU.

étrangères. A cet égard, nous nous sommes limités aux enseignements tirés:

1) de la pratique des assurances françaises, pratique fondée sur la loi du 6 janvier 1978 et surtout sur la norme simplifiée n° 16 concernant « les traitements automatisés d'informations nominatives relatives à la passation, la gestion et l'exécution des contrats mis en œuvre par les organismes d'assurances, de capitalisation, de réassurance et d'assistance et par leurs intermédiaires » (6).

2) de la pratique des assurances allemandes telle qu'elle se déduit des principes de la Bundesdatenschutzgesetz et d'une abondante doctrine relative aux problèmes particuliers des fichiers d'assurance (7).

3) de la pratique des assurances américaines établie par le « Insurance Information and Privacy Protection Model Act » approuvé en 1979 par la « National Association of Insurance Commissioners » (NAIC) (8), sorte d'office de contrôle des Assurances. Ce Model Act a été approuvé à l'heure actuelle par une vingtaine d'Etats.

4. L'objet de notre propos ainsi précisé, comment l'aborder? Certaines notions de base nous paraissent devoir être présentées avant d'analyser les différents aspects du fonctionnement du fichier.

Trois notions fondamentales permettent en effet la compréhension des règles de fonctionnement des fichiers d'assurances;

(6) La norme n° 16 a été établie par la CNIL le 20 janvier 1981 (publiée au Journal officiel, le 5 février 1981) suite à des contacts avec les représentants des sociétés d'assurances. Elle représente une application de l'article 17 de la loi française qui stipule:

« Pour les catégories les plus courantes de traitements à caractère public ou privé qui ne comportent manifestement pas d'atteinte à la vie privée ou aux libertés, la Commission nationale de l'informatique et des libertés établit des normes simplifiées inspirées des caractéristiques mentionnées à l'article 19 ».

« Pour les traitements répondant à ces normes, seule une déclaration simplifiée de conformité à l'une de ces normes est déposée auprès de la commission. Sauf décision particulière de celle-ci, le récépissé de déclaration est délivré sans délai. Dès réception de ce récépissé, le demandeur peut mettre en œuvre le traitement. Il n'est exonéré d'aucune de ses responsabilités.

(7) Parmi l'abondance doctrine allemande, signalons plus particulièrement, S. Simitis, U. Damman, O. Mallman, H.J. Rch, Kommentar zum Bundesdatenschutzgesetz, 3^e éd., Nomos, Baden-Baden; D. Biesalski, Datenverarbeitung im Konzern, B.B., 1978, 67 et s. En particulier, pour le secteur des assurances, P. G. Mohr, Probleme des Datenschutzes in der Versicherungswirtschaft, Z. Ges. Vers. W., 1978, 43 et s.; E. von Ucker-mann, Auswirkungen des Datenschutzes auf die Versicherungswirtschaft, Der Versicherungs-vertrieb, 6/1976, 3 et s.

(8) Le texte est commenté in Privacy Protection Law and the United States, NTIA Report 82-98, U.S. Department of commerce (texte repris en annexe n° 1).

il s'agit de la notion centrale de « fichier », de celle ensuite du « fiché », de celle enfin de « ficheur », si je puis me permettre ce néologisme.

Quant aux différents aspects du fonctionnement abordés par toute réglementation, il s'agit de distinguer :

- les règles de création du fichier;
- les règles précisant le contenu du fichier;
- les règles régissant la collecte des données;
- les règles établissant le droit d'accès des fichés;
- les règles définissant le droit d'utilisation interne et externe des informations reprises;
- enfin les règles organisant le contrôle du bon fonctionnement du fichier.

I. LES NOTIONS FONDAMENTALES

A. Le fichier

5. Dans quelle mesure, une collecte d'informations doit-elle être assujettie à des règles particulières ?

Doit-on mettre sur le même pied, le fichier manuel et le traitement automatisé de données ? L'ex-projet Vanderpoorten (9) soulignait que seules les capacités de l'ordinateur expliquaient le franchissement d'un seuil « qualitatif » dans le traitement des données et faisaient craindre pour nos libertés. Sur base de ce principe, la majorité des réglementations étrangères (10) ne s'applique qu'aux seuls traitements entièrement automatisés.

A cet égard, le projet belge s'il ne s'applique qu'aux traitements automatisés, donne à ceux-ci une définition large qui peut faire craindre quelques difficultés d'interprétation. Au sens du projet, le traitement automatisé est « tout ensemble d'opérations réalisées en tout ou en partie à l'aide de procédés automatisés et relatifs à l'enregistrement, la conservation, la modification, l'effacement, l'extraction ou la diffusion de données à caractère

(9) Projet de loi relatif à la protection de certains aspects de la vie privée, Doc. parl., Sénat, 1975-1976, 846, n° 1, Exposé des motifs.

(10) Danemark, n° 294, § 1 (2); Conseil de l'Europe, art. 2 b); Autriche, art. 2, § 3, 1; Suède, § 1; Luxembourg, art. 2. Contra: Norvège, § 1 et Allemagne, § 2 (3), 3.

personnel, ainsi que l'application à celles-ci d'opérations logiques ou arithmétiques » (11).

Ainsi, les fichiers même manuels des compagnies d'assurances pourront être soumis aux dispositions de la loi du moment que leur utilisation s'appuie même occasionnellement sur un traitement automatique des informations (12). Cette solution est lourde : la compagnie d'assurances sera tenue à déclarer le contenu de tous ces fichiers, le fiché doit y avoir accès. A la limite, la volonté des assurances de conserver, pour des raisons de confidentialité et de sécurité, certaines données sensibles (notamment des données médicales) sur des fichiers manuels mieux protégés est combattue.

Dans la mesure où le législateur belge craint certains abus dans le traitement des fichiers manuels, sans doute aurait-il intérêt à adopter la solution française (13) plus souple qui n'applique à certains fichiers manuels désignés par la Commission que les dispositions relatives à la collecte et au contenu des fichiers mais non celles relatives à la création du fichier, au droit d'accès du fiché...

6. La notion de « traitement automatisé » pose une seconde question. Par traitement automatisé, faut-il entendre tout programme, tout fichier, ce qui obligerait chaque entreprise d'assurance à établir autant de déclarations qu'elle ne dispose de fichiers et de programme de gestion de ces fichiers ou peut-on pour reprendre la terminologie des gestionnaires de grandes organisations n'envisager que les « systèmes d'informations » pour lesquels peuvent intervenir de multiples programmes et applications (14).

(11) Art. 14, § 1 du projet belge. On notera que les mots incriminés « en tout ou en partie » n'étaient pas présents dans les premières versions du projet.

(12) Ainsi, il suffirait qu'un dossier manuel contienne un numéro d'abonné ou de sinistre faisant l'objet d'un traitement automatisé pour être soumis à la loi.

(13) Art. 45, alinéa 1, de la loi française. Ajoutons que l'alinéa 3 du même article permet au gouvernement sur proposition de la CNIL et par décret en Conseil d'Etat d'étendre certaines dispositions de la loi à certains fichiers « qui présentent soit par eux-mêmes, soit par leur combinaison de leur emploi avec celui d'un fichier informatisé, des dangers quant à la protection des libertés » (à ce propos, lire le commentaire de P. Kayser et J. Frayssinet, Informatique et libertés, J. cl. dr. pénal, Annexes 1981, n° 107 et 108).

(14) Ainsi, à la limite, chaque compagnie d'assurance constituerait un seul système d'information disposant de multiples applications, application : gestion interne, application : facturation, applications : dossiers assurance, responsabilité civile, dossiers assurance soins de santé, etc.

La pratique étrangère des lois relatives à la protection des données (15) permet de résoudre cette question technique. Par traitement, il faut entendre le niveau intermédiaire entre le simple programme et le système d'information, celui de l'« application », qui en informatique, s'entend de l'ensemble des informations et des logiciels qui concourent à la mise en œuvre d'une « fonction principale donnée », ce qui peut bien évidemment comprendre de multiples fichiers et de nombreux programmes « enchaînés » (16).

B. Le fiché

7. le projet belge entend par données « à caractère personnel » les données relatives à une personne physique identifiée ou identifiable » (17). Il exclut donc du champ d'application de la loi les données relatives aux personnes morales au nom de la transparence nécessaire des activités commerciales et industrielles (18). Nous avons critiqué cette exclusion et suggéré à ce propos certaines distinctions (19). Sans revenir à ces critiques, notons que certaines fiches relatives à des personnes morales ou associations contiennent bien évidemment des données relatives à des personnes physiques. Ainsi, on imagine mal qu'une société d'assurance-crédit ne reprenne pas, à propos des sociétés assurées, certaines informations quant à la qualité des dirigeants de cette société.

Il est unanimement admis que les réglementations applicables aux seules données relatives à des personnes physiques s'étendent à de telles informations même si celles-ci ne font pas l'objet

(15) Cf. à ce propos, déjà le premier rapport de la CNIL (1978-1980), la documentation française, p. 25 et s.; Cf. également U. Damman, op. cit., n° 186 et s.

(16) Ainsi, une application informatique en matière de responsabilité véhicules terrestres automoteurs peut selon l'organisation et le mode de réalisation adoptés par les informaticiens de l'entreprise comprendre outre le fichier « clients », le fichier « sinistres », le fichier documentaire relatif aux solutions jurisprudentielles, le fichier « courtiers » ou « agents », les programmes de gestion de ces différents fichiers, des programmes permettant l'élaboration de statistiques, un programme permettant le calcul d'une proposition de couverture.

(17) Art. 14, § 2.

(18) Sur ce point, outre l'exposé des motifs du projet (p. 77), les remarques de Mr Spreutels, art. cité, p. 7, n° 8.

(19) P. et Y. Pouillet, *Applicabilité aux entreprises d'une législation - protectrice des données*, Banque de données Entreprises - Vie privée, Actes du colloque de Namur, CIEAU, CREADIF, 1980, 237 et s. (avec un état de la législation et de la doctrine en la matière).

d'un traitement ou d'un fichier individualisé (20). Ce principe peut présenter lors de son application pratique certaines difficultés pour les entreprises d'assurances ne distinguant pas nettement dans leurs systèmes d'informations relatifs aux personnes morales les fichiers relatifs aux personnes physiques et ne permettant pas d'accès direct à ces fichiers.

C. Le « ficher »

8. La dernière notion est certes la plus délicate à traiter. Qu'entend-on, au sens des différentes réglementations, par ficher ? Faut-il s'en référer à la notion de personne juridique et considérer qu'est tiers, les personnes juridiques ayant une personnalité juridique distincte de celle du ficher en question ? Ceci amènerait à distinguer par exemple, les filiales tiers et les succursales non tiers par rapport à la société, leader d'un groupe; faut-il estimer qu'une même personnalité juridique peut constituer différents fichers ou, à l'inverse, reconnaître, au nom de l'unité économique d'un groupe, que plusieurs personnalités juridiques peuvent constituer un seul et même ficher ?

Le problème est d'importance dans le secteur des assurances. Si les associations belges d'assurances mutuelles sur la vie sont constituées en droit belge (21) comme dans bien d'autres pays sous forme de sociétés coopératives ayant une personnalité juridique indépendante, en ce qui concerne les autres « branches » de l'assurance (22), celles-ci peuvent selon la politique propre à chaque groupe, constituer plusieurs sociétés suivant les diverses branches ou au contraire concentrer en une seule société leurs différentes activités (sociétés multibranches).

En ce qui concerne la production, on distinguera de même l'activité des courtiers ou d'agences constitués sous forme de sociétés indépendantes et celle d'agents simples employés ou succursales de sociétés d'assurances.

(20) A cet égard, les remarques de Joinet, *Informatique et libertés*; approche du problème par les autorités gouvernementales, *Computer in privacy*, Leuven, 1976, 81; Rapport Bayerl au Parlement de la Communauté, p. 27; U. Damman, op. cit., § 2, n° 7 et s. et les références y reprises.

(21) Loi du 25 juin 1930 relative au contrôle des entreprises d'assurances sur la vie, art. 7.

(22) L'annexe I de la loi du 9 juillet 1975 relative au contrôle des entreprises d'assurances distingue 20 branches d'activités. On notera que l'article 14 de la même loi oblige les entreprises à établir une gestion et une comptabilité distinctes par branche ou groupe de branches. L'alinéa 3 prescrit même l'obligation pour les entreprises de tenir une liste, un fichier ou tout autre répertoire des contrats et des sinistres par gestion distincte.

9. Quelles conséquences, le projet attache-t-il à ces distinctions et quelle définition retient-il en définitive? Comme d'autres législations, en particulier l'allemande (23), le projet envisage différemment l'utilisation interne d'une information et la communication à un tiers, cette dernière faisant l'objet de contrôle plus sévère. Comme on aura l'occasion de le voir plus loin (infra n° 16), les entreprises qui se servent de l'information à des fins purement internes sont dispensées de toute une série de prestations: devoir d'avertissement du fiché lors du premier enregistrement (art. 22 § 1), devoir d'information de celui-ci lors de la collecte d'informations (art 17), possibilité d'autoriser par arrêté royal des déclarations simplifiées (art. 26 § 6). Il est donc utile de préciser la notion de tiers.

Le tiers est défini par le projet comme étant «toute personne physique ou morale, de droit privé ou de droit public, autre que la personne physique ou morale ou tout organisme, non doté de la personnalité juridique, compétents pour décider de la finalité du traitement automatisé, des catégories de données à caractère personnel enregistrées ou des opérations de traitement automatisé qui leur sont appliquées» (24).

10. Sans parler ici des nombreuses difficultés d'interprétation auxquelles conduit cette définition appliquée au secteur public (25), une telle définition de la notion de tiers risque, dans le secteur privé des assurances, de créer quelque embarras et une discrimination au profit des sociétés multibranches.

En effet, une société multibranches constitue-t-elle un seul ficheur ou doit-on admettre suivant le principe de la division des risques, principe, me semble-t-il, voulu par le législateur, qu'il y a autant d'entreprises que de branches et qu'entre ces entreprises les données circulent moins librement? Cette seconde solution est celle de la législation allemande (26). Elle s'appuie dans ce pays sur le fait que la loi impose la constitution de sociétés indépendantes par branche d'activités (27). A suivre le projet

(23) Sur ce point, nos réflexions infra n° 11.

(24) Article 14, § 3, al. 1°.

(25) Sur ce point, nos réflexions in le droit à la vie privée selon le projet Gol, J.T., 1982, n° 5230, p. 769, n° 4.

(26) A ce propos, P.G. Mohr, art. cité, 48; V. Biagosh, Datenschutz und Datensicherung in der Wirtschaft, Der Versicherungsbetrieb, 77, 13 et 14, T. Elbra, rapport cité, 41.

(27) On notera cependant que la transmission des données est envisagée plus libéralement en Allemagne qu'en Belgique, en particulier dans les groupes de sociétés. Sur ce point, les remarques de Simitis, Bundesdatenschutzgesetz - Ende der Diskussion oder Neubeginn?, NJW, 1977, 733-734.

belge, une solution différente s'imposerait en Belgique à moins qu'un juge n'estime que chaque branche constitue, selon l'expression du projet, un organisme compétent pour décider de la finalité du traitement automatisé (28).

A ce propos, il nous apparaît qu'il faut tenir compte de deux intérêts conciliables, premièrement, celui des entreprises d'assurances de pouvoir communiquer entre leurs divers services des informations générales relatives aux assurés (identité, adresse, n° de police,...), secondement, celui des fichés de ne pas voir les compagnies d'assurances concentrer en une seule base de données tous les renseignements tirés des différentes branches d'activité de cette compagnie. Ainsi, la norme simplifiée française n° 16 déjà évoquée distingue des informations valables pour l'ensemble des types d'assurance (29) et certaines propres à certains types d'assurance qui ne peuvent être traitées et conservées que dans des fichiers propres et avec des clés d'accès propres (30).

11. Une dernière précision a trait au type de «ficheur» que constitue une société d'assurances, selon les diverses législations. On fait ici allusion à la classification opérée par la loi allemande

(28) Dans le projet Moureaux dont s'est fortement inspiré le projet Gol (cf. sur ce projet E. Lentzen, Fichiers nominatifs et vie privée, Courrier hebdomadaire du CRISP, n° 948-949, 5 février 1982, 44 à 54), la notion de tiers était définie par rapport à la notion de maître du fichier (art. 13). La notion était définie comme suit: «la personne physique ou morale, l'autorité publique, le service ou tout organisme qui est compétent selon la loi nationale, pour décider quelle sera la finalité du fichier automatisé, quelles catégories de données à caractère personnel doivent être enregistrées et quelles opérations leur seront appliquées» (cf. dans le même sens, la définition du Conseil de l'Europe art. 2 d)).

Cette notion ne permet pas d'y voir plus clair. En effet, il suffit de décider que dans une société multibranches toute décision d'informatisation relève du conseil d'administration de la société.

Un argument pourrait être avancé dans le sens de l'autonomie de chaque branche. L'article 14, § 3, alinéa 2, précise que ne sont pas des tiers les catégories de personnes qui à raison de leurs fonctions ou pour les besoins du service, ont directement accès aux informations enregistrées. A contrario, ne peut-on déduire que constitueraient des tiers même s'ils relèvent de la même société des personnes étrangères au service, pour lequel l'information a été enregistrée, ainsi les personnes préposées au service «Responsabilité civile véhicules terrestres» par rapport à celles préposées au service «Maladie».

(29) Ainsi, l'identité, la situation économique et financière (revenus annuels, profession, identité bancaire, frais généraux), les informations nécessaires à l'application des contrats, les informations relatives à la détermination du préjudice.

Parallèlement, le législateur allemand prévoit la libre circulation de données neutres: nom, titre, date de naissance, profession, adresse, numéro de téléphone (B.D.S.G., § 24, al. 2). Sur ce point, von Uckermann, Das Bundesdatenschutzgesetz und die Versicherungswirtschaft, V.W., 1977, 437.

(30) Ainsi, par exemple les assurances de personnes et de responsabilité civile (à propos des données relatives à la santé, à la situation familiale, à la formation, aux loisirs).

et suivie par d'autres législations (31) et aux conséquences importantes tirées de cette classification

La législation allemande distingue trois types de fichiers :

- les fichiers du secteur public;
- les fichiers du secteur privé agissant pour leur propre compte;
- les fichiers du secteur privé agissant pour le compte de tiers dans le domaine commercial.

Les règles applicables à ces différentes catégories de fichiers divergent profondément. L'Etat puise son droit à l'information dans la nécessité de pourvoir à des besoins collectifs. Les principes de légalité, de spécialité et la transparence du parc informatique du secteur public apparaissent comme le corollaire de ce droit dans une société démocratique.

Lorsque l'entreprise travaille pour compte propre, « c'est dans le rapport synallagmatique (ou quasi contractuel) qui s'établit entre l'entreprise et son client que se trouve le fondement juridique de la collecte (du traitement et de la communication) de l'information » (32). Ce principe justifie une réglementation plus souple des fichiers de cette seconde catégorie. L'article 23 de la loi allemande prescrit que

« La mémorisation de données d'identification personnelle est autorisée dans le cadre des finalités d'un rapport contractuel ou d'un rapport de confiance quasi contractuel avec la personne concernée, pour autant que cette même mémorisation soit indispensable à la sauvegarde des intérêts légitimes de l'instance mémorisatrice et à condition qu'il n'y ait pas lieu de supposer que cette même mémorisation porte atteinte aux intérêts légitimes de la personne concernée ».

L'article 24 envisage, dans le même esprit, la transmission des données :

« La transmission de données d'identification personnelle est autorisée dans le cadre des finalités d'un rapport contractuel ou d'un rapport de confiance quasi contractuel avec la personne concernée ou dans la mesure où cette même transmission est indispensable à la sauvegarde d'intérêt légitime de l'instance divulgateuse ou d'un tiers ou de la collectivité et à condition qu'elle ne porte pas atteinte aux intérêts légitimes de la personne concernée ».

(31) En particulier, les législations autrichiennes et danoises.

(32) Rapport Tricot, La documentation française, Paris, 1975, T. II, p. 192.

Quant aux entreprises ayant pour objet de commercialiser des informations (bureaux de renseignements sur le crédit et l'emploi, éditeurs d'adresse mais également les associations professionnelles autorisées à prévenir les compagnies d'assurances en cas de risques), elles constituent leur fichier non seulement en dehors de tout rapport avec le fiché mais en outre de tout service à rendre à ce dernier. On conçoit dès lors qu'une réglementation plus stricte, par le biais d'un contrôle a priori, par l'extension du droit d'accès des fichés de limitation dans le temps de la conservation des données, gouverne leurs activités.

Les jurisprudences et doctrines allemandes sont unanimes à classer toutes les entreprises d'assurances y compris les sociétés de réassurance dans la seconde catégorie et d'appliquer dès lors les principes plus souples rappelés ci-dessus. Lors de l'analyse du fonctionnement des fichiers, nous aurons, à plusieurs reprises, l'occasion de souligner tout l'intérêt de l'approche allemande.

12. Les différents prescrits du projet belge permettent-ils de dégager une classification semblable et d'en tirer certaines conséquences. A première vue, non. On sait que le projet actuel, à l'inverse du projet Vanderpoorten, ne distingue pas entre les banques de données du secteur privé et celles du secteur public et envisage de façon presque uniforme la réglementation de tous les fichiers. Le libellé d'une seule exception nous permettrait cependant d'appuyer la distinction allemande entre fichiers constitués pour compte propre et ceux ayant pour objet la commercialisation d'informations. En effet, à plusieurs reprises, le projet dispense de lourdes obligations (33) les entreprises collectant et traitant des données « qui ne sont pas destinées à être communiquées à des tiers » (34). L'interprétation de l'exception ainsi libellée est loin d'être évidente (35). Ainsi, la plupart des informations

(33) Ainsi, celle de donner au fiché ou à un tiers toute une série d'informations lors de la collecte des données (cf. infra, n° 16); celle d'informer le fiché lors du premier enregistrement le concernant (cf. infra, n° 19); celle de bénéficier de la possibilité de déclarations simplifiées (cf. infra, n° 13).

(34) Cf. déjà les ambiguïtés de la notion de tiers dénoncées, supra, n° 8.

(35) ... d'autant plus que l'article 31 relatif aux dispositions pénales complémentaires utilise les mêmes termes « Est puni... celui qui a communiqué à un tiers une donnée à caractère personnel figurant dans un traitement automatisé en sachant qu'elle n'était pas destinée à être communiquée à des tiers ». Il semble que cet article 31 ne puisse cependant servir à l'interprétation de la notion en question, nonobstant l'emploi des mêmes termes. Le « traitement de données non destinées à être communiquées à des tiers » envisage la finalité des données collectées a priori : sont-elles ou non reprises pour une utilisation interne ? La disposition pénale sanctionne la transmission non autorisée et consciente d'une donnée, peu importe la finalité a priori du traitement. Quoiqu'il en soit, les termes et leur interprétation devraient être précisés dans la loi ou, à défaut, dans l'exposé des motifs. On regrette l'absence actuelle de précision en cette matière importante.

récoltées par une société d'assurance peuvent, à l'occasion d'un sinistre ou d'une réassurance voire de la transmission à un agent ou à un courtier par exemple, être communiquées à des tiers. Sont-elles pour autant « destinées à être communiquées à des tiers » au sens du projet ? Il nous apparaît que non. Le cas des sociétés d'assurance-crédit fréquemment appelées par des tiers pour couvrir des risques de crédit est moins clair, encore qu'à strictement parler, la société d'assurance-crédit ne communique pas comme telles les données aux tiers mais simplement sa décision de couvrir ou non le crédit proposé et ce sur base des données dont elles disposent. Plus délicat encore, le cas des centrales de renseignement établies au sein de l'UPEA par les compagnies d'assurances elles-mêmes et ayant pour but de dépister les mauvais risques ou d'éviter de doubles assurances.

Dans ce dernier cas, il semble bien que la finalité du traitement soit la communication de données à des tiers et qu'il y ait donc traitement de données destinées à être communiquées à des tiers.

En toute hypothèse, il serait souhaitable que le projet si telle est bien son intention distingue plus clairement, à l'instar de la législation allemande, d'une part, les réglementations des fichiers constitués pour compte propre parmi lesquels figurent l'ensemble des fichiers d'assurance et, d'autre part, la réglementation de fichiers commercialisés.

II. LE FONCTIONNEMENT DES FICHIERS

A. La création du fichier

La création d'un traitement automatisé de données nominatives ne peut, selon le projet, rester secrète. Déclaration (36) sur son contenu, son fonctionnement et la technique utilisée doit être

(36) L'article 26 stipule que « la déclaration doit être faite par la personne physique ou morale..., ou l'organisme non doté de la personnalité juridique compétents pour décider de la finalité du traitement,... » sans préciser outre mesure la fonction : qui au sein d'une société est tenu d'établir la déclaration et serait responsable de son exactitude (dans le même sens, les remarques du Conseil d'Etat, p. 28). Mr. Spreutels (op. cit., n° 10, p. 9) s'en réfère au système de l'imputabilité judiciaire qui laisse au juge le soin de déterminer le véritable responsable.

faite au Ministre de la Justice (37). Cette déclaration est éventuellement (38) simplifiée pour les traitements de données qui ne sont pas destinées à être communiquées à des tiers (39). Elle est

(37) Art. 26 § 1.

Le § 2 de l'article 26 précise le contenu de la déclaration, elle comprend 16 mentions

- dont 9 sont reprises au registre public :

- 1° la date de sa déclaration et, le cas échéant, la mention de la loi, du décret ou de l'acte réglementaire décidant sa création;
- 2° les noms, prénoms et adresse complète ou la dénomination et le siège des déclarants;
- 3° la dénomination du traitement automatisé;
- 4° le but poursuivi par le traitement automatisé;
- 5° l'objet des données à caractère personnel qui sont traitées, ainsi que la justification du choix de ces données eu égard au but poursuivi;
- 6° les catégories de personnes admises à obtenir les données;
- 7° les conditions de communication des données aux personnes visées au 6°, ainsi que les conditions d'utilisation des données qui sont communiquées;
- 8° les moyens par lesquels les personnes font l'objet des données en seront informées, le service auprès duquel s'exercera le droit d'accès, les mesures prises pour faciliter l'exercice de ce droit;
- 9° la période au-delà de laquelle les données ne peuvent plus, le cas échéant, être gardées, utilisées ou diffusées.

En outre, sept informations supplémentaires figureront dans la déclaration :

- 1° les modes de collecte des données à caractère personnel;
- 2° le système de traitement automatisé choisi;
- 3° les méthodes d'application du traitement automatisé des données;
- 4° le service ou les services chargés de mettre en œuvre le traitement automatisé;
- 5° les rapprochements, les interconnexions ou toute autre forme de mise en relation des données, ainsi que les conditions auxquelles celles-ci pourront éventuellement être cédées à des tiers;
- 6° les catégories de personnes qui, à raison de leurs fonctions ou pour les besoins du service, ont directement accès aux informations enregistrées;
- 7° les systèmes de sécurité et de contrôle à mettre en place en vue d'assurer l'intégrité des données, de prévenir ou de détecter une utilisation des données qui ne serait pas conforme à leur destination.

On relèvera qu'aucune législation étrangère (y compris la législation suédoise) ne prescrit une déclaration aussi complète. Les législations allemande, danoise, autrichienne et américaine dispensent les banques de données travaillant pour compte propre (supra n° 10) d'une telle déclaration. Cette remarque prend tout son sens lorsqu'on sait qu'en pratique, tous les organes de contrôle à l'étranger sont débordés.

(38) le projet belge suit l'exemple de la loi française. On relèvera cependant :

- 1° que le prononcé de ces déclarations simplifiées est, en France, le fait de la CNIL; en Belgique, le fait du Roi après avis de la commission consultative de la vie privée et décret en Conseil d'Etat;
- 2° que ces déclarations visent, en France, des catégories courantes de traitements ne comportant manifestement pas d'atteinte à la vie privée et aux libertés, en Belgique, les traitements de données « qui ne sont pas destinées à être communiquées à des tiers ».

(39) Sur les ambiguïtés de cette notion, supra, n° 10; En Allemagne, les banques travaillant pour compte propre ne sont soumises à aucune déclaration mais leurs gestionnaires tiennent un « état » de leurs fichiers.

complétée (40) en cas de transmission même occasionnelle (41) et quel que soit le support utilisé vers l'étranger des données recueillies. Enfin, l'article 26 § 5 prévoit sa mise à jour.

De cette déclaration, les fonctionnaires du Ministre de la Justice extrairont certains renseignements (42) qu'ils consigneront dans un registre public. A nouveau, certains traitements d'informations non destinées à être communiquées à des tiers peuvent être dispensés de l'inscription de certaines indications.

L'article 25 du projet évoque en outre les responsabilités du gestionnaire du fichier, c'est-à-dire de celui qui gère effectivement le matériel et les programmes mais n'en prévoit pas la nomination par la personne compétente pour décider de la finalité du traitement comme le faisait le projet Moureaux.

Ce gestionnaire peut-il être un tiers, c'est-à-dire une personne étrangère aux services de l'entreprise, maîtresse du fichier, ainsi par exemple un service-bureau travaillant notamment pour le compte d'un courtier? Si tel est le cas (43), on peut se demander qui sera responsable en cas de déclarations inexactes ou de non respect de la réglementation. En particulier, faut-il admettre une responsabilité civile solidaire du gestionnaire et du maître du fichier, comme le prévoyait l'ancien projet Vanderpoorten (44)?

B. Le contenu du fichier

14. A l'approche positive déjà mentionnée de la loi allemande (supra n° 11) et pratiquée par la Commission française Natio-

(40) Article 26, § 4: La déclaration précise les catégories de données, objet de la transmission, le pays de destination et le pays par l'intermédiaire duquel la transmission s'effectuera (ce qui risque déjà d'être difficile dans le cas de transmission par les réseaux télématiques, plus encore dans le cas de transmission par satellites).

(41) Beaucoup de compagnies d'assurances seront tenues par cette déclaration, dans la mesure où les compagnies de réassurances sont bien souvent situées à l'étranger.

(42) L'article 27, § 2 précise les neuf mentions reprises au registre (cfr. sur la liste des données «enregistrées» supra note (37)).

(43) Seule, la loi norvégienne propose une réglementation particulière aux services bureaux (chapitre 6, § 22 et s.). La pratique fréquente du travail par l'intermédiaire de service-bureau pose quelques questions. Ainsi, constituent-ils au sens de l'article 26 § 2 6° «une catégorie de personnes qui à raison de leurs fonctions ou pour les besoins du service ont directement accès aux informations enregistrées» ou sont-ils des tiers?

(44) Article 24 du projet: «Le maître du traitement automatisé et le gestionnaire répondent solidairement de tout dommage résultant d'infractions aux dispositions de l'article 23 de la présente loi».

nale Informatique et Libertés (45) on opposera l'approche négative du projet belge (46). Le rapport Tricot préalable à l'adoption de la loi française (47) estime que «le service attendu de l'entreprise est à la fois la justification et la limite de l'usage des renseignements».

Dans ce pays, c'est l'application du principe de «pertinence» mis en évidence par le Conseil de l'Europe (48). Les données personnelles doivent être enregistrées pour un but légitime et déterminé et ne doivent pas être utilisées en contradiction avec ce but, elles doivent convenir aux buts pour lesquels elles sont enregistrées, être déterminantes par rapport à la réalisation de ce but et non superflues. Elles doivent être exactes et si nécessaire, mises à jour. Enfin, elles doivent être effacées lorsqu'elles ne sont plus nécessaires à la réalisation du but poursuivi...».

Le projet belge, quant à lui, après avoir affirmé le principe du respect de la vie privée (49), définit un certain nombre de données «interdites», ainsi les origines raciales ou ethniques, les appartenances syndicales ou mutualistes (50), les données à caractère personnel relatives à la vie sexuelle, aux opinions ou activités politiques, philosophiques ou religieuses. L'obtention d'un

(45) A noter en ce sens, les conclusions de l'étude de F. Chamoux, J.P. Chamoux, H. Delahaie, La loi «Informatique et libertés» face aux entreprises, Computerrecht, 1984 n° 1, pp. 3 à 9.

(46) Sur cette différence d'approche, nos réflexions in L'informatique menace-t-elle nos libertés? in La télématique, Aspects techniques, socio-politiques et juridiques, Actes du colloque de Namur 5 et 6 décembre 1983, Gent, éd. Story-Scientia, vol 1, pp. 193 et 194.

(47) Le rapport de la commission «Informatique et libertés» (dit Rapport Tricot), instituée par le décret n° 74 - 938 du 8 nov. 1974 a largement inspiré la loi française du 6 janvier 1978. Il a été publié à la Documentation française en 1975 (2 tomes).

(48) Article 5 de la convention du Conseil de l'Europe du 17 septembre 1980.

Quality of data

«Personal data undergoing automatic processing shall be

- a. obtained and processed fairly and lawfully;
- b. stored for specified and legitimate purposes and not used in a way incompatible with those purposes;
- c. adequate, relevant and not excessive in relation to the purpose for which they are stored;
- d. accurate and, where necessary, kept up to date;
- e. preserved in a form which permits identification of the data subjects for no longer than is required for the purpose for which those data are stored».

(49) A noter la définition donnée par un auteur américain Westin de la notion de vie privée: «the claim of individuals to determine for themselves when, how, and what extent information about them is communicated to others».

(50) Le Conseil d'Etat a fait remarquer qu'«en ce qui concerne l'alinéa 2, il paraît difficile de ranger l'appartenance à une mutualité parmi les opinions ou les activités...». L'exclusion des données mutualistes pose bien évidemment des problèmes insolubles pour les compagnies d'assurances «maladie».

«consentement spécial donné par écrit par l'intéressé» est nécessaire, selon le projet pour le traitement automatique (50bis) de données médicales c'est-à-dire non seulement les données relatives aux examens médicaux mais également les données relatives aux soins et traitements médicaux au sens large (y compris l'alcoolisme ou les autres intoxications). En ce qui concerne les compagnies d'assurance-maladie et les compagnies d'assurance-vie, elles devront dès lors obtenir ce consentement spécial et par écrit. A cet égard, on s'inquiète, une mention même en caractère gras dans un contrat d'assurance ou dans une convocation à un examen médical constitue-t-elle ce consentement spécial ou faut-il une autorisation expresse séparée et révocable décrivant les différents types de données médicales dont l'utilisation serait autorisée? Quid en cas de refus? La solution française telle qu'elle est prévue par la norme n° 16 de la CNIL est plus libérale, elle se réfère aux principes de pertinence (51) et comme la législation allemande (51 bis), rappelle l'obligation de secret professionnel à charge des détenteurs de telles données. On relève encore dans la loi New Yorkaise relative aux assurances (§68a) l'interdiction pour les assureurs de transmettre l'information médicale sauf permission écrite explicite par le fiché.

Le NAIC Model Act américain permet cependant la communication à des institutions médicales ou professionnelles lorsqu'il s'agit de vérifier la couverture d'un individu ou de l'informer d'un problème médical (section 13).

15. Le problème posé aux assureurs belges par les restrictions d'utilisation des données médicales existe également en ce qui concerne les données «du passé judiciaire» parmi lesquelles l'article 20, § 1, 1° comprend «les infractions... pour lesquelles une personne a été condamnée, ainsi que les peines prononcées à son égard» et l'article 20 § 2 mentionne les litiges soumis aux cours et tribunaux. En principe, leur traitement automatique est interdit. L'article 20 § 3 prévoit une exception qui peut s'appliquer aux compagnies d'assurances (52). « Moyennant avis donné par

(50bis) Rappelons le sens large donné par le projet à la notion de traitement informatique.

(51) Cf. La norme simplifiée n° 16 qui stipule, à propos des assurances de personnes et de responsabilité civile, la possibilité de prendre des informations relatives à la santé dans la mesure où ces éléments sont nécessaires à la passation, à la gestion et à l'exécution des contrats.

(51 bis) Art. 24 (1), 2° alinéa. Cet article exclut leur communication mais permet aux compagnies leur traitement automatisé.

(52) ... comme le prévoit expressément l'exposé des motifs (p. 21), ces dérogations pourront «être accordées, en vue de sauvegarder des intérêts légitimes, tels que la sécurité du crédit ou le bon fonctionnement des entreprises d'assurances».

écrit à l'intéressé, tout ou partie de données à caractère personnel énoncées aux § 1 et § 2 peuvent toutefois figurer dans des traitements automatisés ou catégories de traitements automatisés, gérés par des personnes physiques ou morales de droit public ou de droit privé, désignés par arrêtés royaux délibérés en Conseil des Ministres, après avis de la Commission consultative de la vie privée...»

On déplorera certes le peu de souplesse, la lourdeur et le manque d'adaptabilité de cette procédure aux besoins informationnels nouveaux des entreprises puisque «les arrêtés royaux énuméreront limitativement les types de données autorisées, les catégories de personnes autorisées à traiter automatiquement ces données ainsi que l'utilisation (53) qu'elles peuvent en faire». A nouveau, il est certain qu'eût été préférable l'approche positive dont question ci-dessus, ce qui aurait rendu inutile par ailleurs le prescrit de l'article 20 § 6, relative à la durée de conservation des données (54).

C. La collecte des données

16. «La collecte des données se fera par des moyens honnêtes, licites et loyaux». Au-delà de ce principe général affirmé par le Conseil de l'Europe, l'article 17 du projet belge distingue deux types de collecte: celle effectuée auprès de la personne fichée et celle recueillie auprès de tiers. Il prévoit en outre des exceptions.

En toute hypothèse, les personnes auprès desquelles sont recueillies des données nominatives doivent être informées

- 1) du caractère obligatoire ou facultatif des réponses;
- 2) des conséquences du refus;
- 3) du but poursuivi par la collecte;
- 4) des catégories de personnes admises à obtenir les données.

Si la collecte est effectuée auprès de la personne fichée, celle-ci sera informée en outre de son droit d'accès et de rectification des données. Si la collecte est effectuée auprès d'un tiers, ainsi une compagnie d'assurance-crédit qui dans le cadre de la couverture d'un crédit bancaire demande des renseignements à la banque sur le client assuré, l'information est due au client de la même façon.

(53) l'emploi du mot «utilisation» signifie-t-il que seule une utilisation interne de ces données est possible et non la communication à des tiers.

(54) «Les données énoncées au § 1 doivent être effacées lorsque leur maintien a cessé de se justifier. Ce § 6 a été ajouté à la demande expresse du Conseil d'Etat.

Les questionnaires standards proposés par les compagnies d'assurance devront-ils obligatoirement mentionner les différentes mentions énoncées ci-dessus? Ce n'est pas évident.

Le § 5 de l'article 17 mentionne une exception à toutes ses obligations, exception dont à notre avis devraient profiter certaines sociétés d'assurances. L'exception s'applique en effet «à la collecte, par les entreprises industrielles ou commerciales, de données à caractère personnel qui ne sont pas destinées à être communiquées à des tiers».

On a déjà noté les difficultés suscitées par les termes «non destinées à être communiquées à des tiers». L'interprétation large conduirait à exonérer des obligations d'information la totalité des compagnies d'assurances, mais non les associations professionnelles d'assurance (c'est-à-dire, chez nous principalement l'UPEA) qui ne peuvent être qualifiées d'entreprises industrielles ou commerciales.

17. A l'étranger, on notera les dispositions plus complètes et précises reprises par la NAIC Model Act américain. Le § 4 du texte oblige les compagnies à informer les preneurs ou bénéficiaires de polices d'assurances de la nature et du but des données nominatives qui peuvent être collectées lors d'un contrat d'assurance, de renouvellement d'une police et d'une modification de la police ou de la prestation. Ces informations doivent être données au fiché préalablement à toute collecte auprès de tiers. Le fiché doit connaître dans ce cas l'existence possible de cette collecte auprès de tiers, le type d'informations qui peuvent être ainsi recueillies et les techniques de collecte. Les compagnies préciseront en outre dans leurs questionnaires les informations collectées qui sont recueillies à des fins de marketing et non de gestion proprement dite du contrat envisagé.

A propos de la divulgation d'information à des tiers (§ 5), le texte prévoit l'obligation de proposer à la signature de l'individu fiché un «statement» spécifiant de façon claire les catégories de personnes autorisées à divulguer l'information, la nature de l'information ainsi divulguée, les buts de cette transmission.

Plusieurs prescrits particuliers concernent les techniques de collecte auprès de tiers, ainsi, le § 22 interdit les «pretext interviews», c'est-à-dire ceux où l'interviewer ne décrit pas clairement qui il est et le but de son interview, sauf si la compagnie d'assurances a raisonnablement des motifs de craindre la fraude ou la réticence des assurés. Le § 7 (a) permet aux compagnies de procéder à un «investigate consumer report» seulement dans les cas où

l'individu sait qu'il peut demander un interview dans le cadre de la préparation de ce rapport et recevoir copie du rapport.

Le rapport NCC remis à la commission des communautés européennes (55) insiste sur l'importance de dispositions relatives à la collecte des données. Elles ont contribué dans les pays où une telle réglementation existe à accroître dans une mesure considérable le sentiment de confiance des fichés dans les systèmes d'information mis en place par les compagnies d'assurances et à permettre à ces dernières de compter sur une information plus fiable. La reconnaissance d'un droit d'accès des fichés aux fichiers contribue encore au renforcement de cette confiance.

D. Le droit d'accès des fichés

18. On sait que le droit d'accès, que nous qualifierons volontiers de «droit à l'image», a de multiples facettes.

A la suite de Mr. Debrulle (55bis), on distinguera :

- le droit de savoir pourquoi on m'interroge (cette première facette a déjà été traitée lors de notre analyse des procédures de collecte);
- le droit de connaître l'existence des banques de données (cette seconde facette n'est rien d'autre que le droit de consulter le registre public analysé, supra n° 13);
- le droit de connaître la banque de données dans laquelle je suis enregistré;
- le droit d'accès proprement dit : pour quels types de fichiers, titulaires du droit, portée, périodicité et coût;
- le droit de contester les données : procédure, charge de la preuve, droit de suite.

Nous nous limiterons aux trois dernières facettes et nous nous contenterons de quelques réflexions à ces propos.

19. Le droit de connaître la banque de données dans laquelle je suis enregistré a été à l'origine de nombreux commentaires, en particulier l'obligation coûteuse pour les fumeurs de notifier immédiatement aux fichés lors du premier enregistrement les concernant, «le but poursuivi par le traitement, les catégories de personnes admises à obtenir les données et les conditions dans lesquelles l'intéressé peut obtenir les renseignements».

(55) Rapport cité, p. 22 et 23.

(55bis) C. Debrulle, Contrôles et sanctions en matière de protection du droit, au respect de la Vie privée, in Banque de données, Entreprises et Vie privée, op. cit., 123 et s.

A cette obligation prévue par l'article 22 § 1, l'article 22 § 6 prévoit une importante exception, celle déjà citée relative « aux traitements automatisés de données à caractère personnel qui ne sont pas destinées à être communiquées à des tiers ». On ne rappellera pas les ambiguïtés de cette notion mais on rapprochera de la formule utilisée par le projet belge, celle plus claire utilisée par le législateur allemand (56): « Si des données sur la personne concernée sont mémorisées pour la première fois, celle-ci doit en être avertie, à moins qu'elle n'ait eu connaissance de la mémorisation par d'autres voies » (57). C'est en effet le principe de la connaissance implicite (58) qui à notre avis devrait justifier l'exonération du devoir d'information dans le chef de certains ficheurs et non le critère peu pertinent de la communication ou non communication à des tiers.

20. Par droit d'accès sensu stricto, on entend le droit pour le fiché de connaître le contenu de la banque de données le concernant et l'utilisation de celui-ci. L'article 22 § 2 (58 bis) permet, à toute personne justifiant de son identité d'obtenir communication, sous une forme aisément compréhensible et ce dans les 30 jours du versement d'une redevance forfaitaire (20 ou 30 D.M en Allemagne).

1°) des données que le traitement automatisé contient à son sujet;

2°) de l'identité des personnes ou des catégories de personnes auxquelles les données ont été communiquées durant les 12 mois précédant la demande;

3°) de la faculté d'exercer les recours prévus... par la loi (cfr. infra n° 21).

En pratique, selon le rapport de Mr. Elbra, seul un fiché sur 1.000 exerce ce droit d'accès auprès des compagnies d'assurances. On notera à ce propos que les assureurs devront communiquer non seulement les données de base collectées mais également

(56) Le législateur français comme bien d'autres législateurs ne prévoit d'information du fiché qu'à la demande de celui-ci.

(57) § 26 (1) du BDSG.

(58) Ainsi le client d'une banque ou l'acheteur à tempérament sait ou doit savoir que son crédit bancaire fait l'objet d'une assurance-crédit.

(58 bis) On notera une exception intéressante proposée par la législation allemande. Il n'y a pas de droit d'accès lorsque la divulgation des données... risque de porter une atteinte grave aux finalités ou aux objectifs de l'instance mémorisatrice ou si des intérêts légitimes prépondérants d'un tiers s'y opposent (cf. art. 26 (4)). Similitis donne, comme exemple, le cas de l'assurance crédit prise par un porteur de créance ne désirant pas que son débiteur connaisse l'existence de la couverture du risque de crédit.

les données résultat (59), qu'ils devront mémoriser les personnes à qui communication a été faite (60). Le NAIC Model Act américain prévoit en outre l'identification des sources d'information (§ 8 (B)) et l'obligation pour le fiché de passer par un médecin pour obtenir les informations reprises dans les fichiers relatifs aux données médicales (§ 8 (C)).

21. Le droit de contester et de rectifier les données incomplètes, inexactes, périmées ou illicites est le corollaire évident du droit d'accès sensu stricto. L'article 23 du projet organise la procédure permettant l'exercice de ce droit.

On note qu'il prévoit une procédure précontentieuse (art. 23 § 3), d'une durée de trente jours. Ce n'est qu'au cas où la demande de rectification, de suppression ou de complément n'a pas été accueillie par le ficheur que la demande pourra être portée devant la juridiction (61). L'action en justice oblige le ficheur à affecter la donnée contestée d'un indice de doute lors de la communication de cette donnée. On notera qu'en Allemagne, elles sont bloquées automatiquement dès leur contestation (art. 27, al. 3 BDSG).

Celle-ci peut lorsqu'il existe des motifs impérieux de craindre la dissimulation ou la disparition des éléments de preuve « ordonner une mesure urgente de nature à éviter cette dissimulation ou cette disparition » (ainsi, il peut ordonner copie des fichiers dans lesquels figurent la ou les données incriminées). Il peut (62) en outre ordonner que communication de la correction ou de la suppression soit adressée aux tiers qui ont reçu communication de l'information incomplète, erronée, périmée ou illicite (art. 25 § 3).

Le projet Moureaux prévoyait expressément qu'au cours de cette procédure, la charge de la preuve de l'exactitude de la donnée incombait au ficheur sauf lorsqu'il était établi que les données contestées avaient été communiquées par le demandeur ou

(59) Ainsi, non seulement les éléments concernant la personne permettant d'apprécier le risque mais également l'appréciation finale. Par contre, ils ne divulgueront pas les renseignements concernant des tiers et traités à l'occasion de l'exécution du contrat passé avec un assuré (ex.: des données relatives à certains clients lorsqu'il s'agit d'assurances responsabilité professionnelle ou d'assurance-crédit).

(60) ... ce qui risque d'être extrêmement lourd, cf., à ce propos, infra, n° 25.

(61) ... l'article 23, § 1, prévoit la compétence du président du tribunal de première instance, siégeant en référé pour toute demande relative au droit en question. Le libellé de l'article 23, § 1, laisse supposer que les juridictions ordinaires restent compétentes.

(62) ... il n'y est pas tenu (cf. contra les solutions luxembourgeoise, française et suédoise).

avec son consentement (63). Il semble que le projet actuel ne reprenne pas ce principe (64).

22. On aura compris l'importance des conséquences techniques qu'entraînera la consécration du droit d'accès (65). Ainsi, les programmes de gestion des données devront permettre l'accès direct à certains types de données et leur blocage, devront mémoriser les communications effectuées; le gestionnaire devra prévoir pour certaines données une place mémoire suffisante de telle sorte que des compléments d'informations puissent s'insérer à la demande du fiché.

E. Le droit d'utilisation des données

23. On distinguera le droit d'utilisation interne à la compagnie d'assurances et celui externe de la compagnie d'assurances vers diverses catégories de tiers.

a. L'utilisation interne

A propos de l'utilisation interne des données, le projet contient peu de dispositions. On a noté qu'il est tenu de désigner le ou les services utilisateurs des données (art. 26), qu'un gestionnaire de la banque de données (art. 25) sera tenu de veiller au respect des dispositions légales et qu'une sanction sévère (art. 31 2°)) punit « celui qui intentionnellement a utilisé un traitement automatique de données à caractère personnel de manière non conforme à la destination de ce traitement ». Par le biais de cette infraction pénale qualifiée de « détournement de finalité », se trouve sans doute consacré indirectement et maladroitement le principe de pertinence qui régit le droit à l'information des fichiers des compagnies d'assurances. Ceci dit, comment savoir s'il y a « détournement de finalité » ? Faut-il comme en France (65 bis) s'en référer à la déclaration où est précisé le but du traitement

(63) Art. 21, § 4 du projet Moureaux: « La charge de la preuve incombe au gestionnaire du traitement automatisé, sauf lorsqu'il est établi que les données contestées ont été communiquées par le demandeur ou avec son consentement ».

(64) Cf. à ce propos J.P. Spreutels, art. cité, n° 50, note 127. Comp. en Allemagne: « les données relatives aux conditions de santé, aux délits, aux infractions ainsi qu'aux opinions religieuses ou politiques doivent être effacées si leur exactitude ne peut être prouvée par l'instance mémorisatrice » (art. 27 (3)).

Comp. le NAIC Model Act qui exige que la compagnie d'assurance notifie les raisons du refus de procéder à la correction, au complément ou à la suppression (§ 9 A).

(65) Sur cette question, E.F.M. Hogrebe, Aspects économiques internationaux de la protection des données, in La confidentialité et la sécurité des données, Rapport à la C.C.E., INRIA, vol. 2, 1980, 416 et s.

ou la juridiction saisie peut-elle condamner pénalement le ficheur lorsqu'elle estime, nonobstant le respect de la déclaration, un enregistrement abusif au regard des intérêts en présence.

La norme simplifiée n° 16 de la CNIL décrit de façon complète les finalités d'un traitement établi par une compagnie d'assurances.

Le traitement ne doit pas avoir d'autres fonctions que :

a) Pour la passation et la gestion des contrats :

- l'étude des besoins spécifiques de chaque demandeur afin de proposer des contrats adaptés à ses risques;

- l'examen et le contrôle du risque;

- la tarification, l'émission des polices et des documents comptables, l'encaissement des primes ou cotisations, leur répartition éventuelle entre les coassureurs, le commissionnement des intermédiaires, la surveillance des risques et les autres opérations techniques nécessaires;

b) Pour l'exécution des contrats :

- les opérations techniques nécessaires, notamment la détermination et le paiement des indemnités et prestations et, s'il y a lieu pour l'apérteur, leur collecte auprès des coassureurs, l'exécution des dispositions prévues au contrat et l'exercice des recours;

- c) L'élaboration des statistiques;

- d) L'établissement de sélections, parmi les clients de l'organisme, pour réaliser des actions de prospection et de promotion liées exclusivement aux activités propres à l'organisme;

- e) L'exécution des dispositions légales, réglementaires et administratives en vigueur.

24. Deux prescrits tirés des législations étrangères méritent d'être cités. Selon la loi française (art. 2), le traitement automatisé des données ne peut être le seul fondement d'une décision à l'encontre du fiché. Il s'agit d'une condamnation claire de pratiques comme celles du credit-scoring ou du « profil de carrière ».

Dans le secteur des assurances, bien des pratiques pourraient être remises en question; ainsi le calcul des primes, la décision d'accorder ou de refuser certaines polices sont parfois entièrement automatisés. La législation française réclame l'intervention d'un jugement humain lors de ces opérations menant à une prise de décision.

Le NAIC Model Act impose d'autres limites à l'utilisation de certaines informations lorsqu'il s'agit de rendre des décisions

négligentes vis-à-vis d'un assuré. La compagnie d'assurances ne peut fonder une décision négative en se fondant uniquement sur des décisions négatives préalables dont la compagnie aurait connaissance par d'autres compagnies ou par une association professionnelle d'assureurs (§ 11).

Cependant, cette information peut être à la base de demandes d'informations complémentaires auprès de la compagnie à l'origine de cette information négative (66).

b. La communication

25. Les compagnies d'assurances vivent d'informations transmises et à transmettre. Si le souscripteur du contrat est certes à l'origine du nombre d'informations, peuvent intervenir également, des experts; les agents ou courtiers indépendants; l'assuré, lorsqu'il est différent des souscripteurs; une autre compagnie d'assurances (en cas de coassurance, de réassurance voire de recours présentés par l'assureur d'une partie adverse); d'associations professionnelles; d'organismes publics enfin (sécurité sociale (67), fonds de garantie (automobile), gendarmerie).

Les destinataires d'informations seront souvent les mêmes personnes, impliquées dans le mode de fonctionnement de l'assurance. Ainsi,

«- les experts missionnés permettent l'évaluation exacte des risques et des sinistres;»

«- par l'intermédiaire des organismes professionnels, les assureurs échangent les informations qui sont de nature à faciliter la prévention et la lutte contre la fraude dont les effets sont préjudiciables aux assurés;»

«- par ailleurs, l'ampleur de nombreux risques contraint les assureurs à recourir à des solutions de répartition telles que la coassurance et la réassurance, qui les conduisent à échanger des informations relatives à ces risques;»

«- dans les opérations de règlement des sinistres, l'assureur doit tenir certaines informations à la disposition des autres assureurs et de ses mandataires. Il peut avoir également à les com-

(66) Sur l'article 2 de la loi française, lire les commentaires de P. Kayser et J. Frayssinet, art. cité, n° 14.

(66bis) Le nom de la compagnie à l'origine de la décision négative sera communiqué au (candidat) assuré.

(67) Sur cette affirmation, cf. l'annexe 2 du second rapport d'activité de la CNIL (1^{er} octobre 1980 - 15 octobre 1980), 238 et s.

muniquer à la sécurité sociale, à la justice et à divers organismes comme les sociétés de recours.»

26. La transmission d'informations à l'intérieur du secteur d'assurances mais même au-delà donc vitale pour les compagnies et nécessaire à leur fonctionnement. Avant d'aborder la solution que le projet belge pourrait apporter à ce problème, notons les solutions étrangères:

- celles américaine (NAIC Model Act) (68) et française (69) qui énumèrent une longue liste de destinataires et les habilite chacun «dans les limites de leurs attributions respectives» (70). Ces réglementations américaine et Française fondent sur une analyse du fonctionnement de l'ensemble d'un secteur d'activités. Dans les deux pays, la réglementation a d'ailleurs été conçue avec les représentants du secteur visé.

- celles, déjà signalées, des pays germaniques suivant lesquels «la transmission des données d'identification personnelle est autorisée dans le cadre des finalités d'un rapport contractuel ou d'un rapport de confiance quasi-contractuel avec la personne concernée ou dans la mesure où cette même transmission est indispensable à la sauvegarde d'intérêts légitimes de l'instance divulgateur

(68) Ainsi lorsque les organismes d'assurances offrent des garanties complémentaires à celles des régimes sociaux.

(69) Section 13 of the NAIC Model Act.

(70) Norme simplifiée n° 16

Peuvent seuls, dans les limites de leurs attributions respectives, être destinataires des informations afférentes à chaque type de garantie:

- les personnels chargés de la passation, la gestion et l'exécution des contrats;
- l'apporteur du contrat (agents, courtiers...) et son personnel;
- les souscripteurs, les assurés et les bénéficiaires des contrats;
- s'il y a lieu, l'organisme d'assurance des responsables de l'accident ou offrant des prestations complémentaires;
- s'il y a lieu, les coassureurs et réassureurs ainsi que les organismes professionnels chargés de gérer le contrat ou de prévenir et de combattre la fraude;
- s'il y a lieu, les avocats, experts, médecins et notaires;
- les caisses de sécurité sociale lorsque les régimes sociaux interviennent dans le règlement des sinistres ou lorsque les organismes d'assurances offrent des garanties complémentaires à celles des régimes sociaux;
- s'il y a lieu, le responsable, les victimes de l'accident et leurs mandataires;
- s'il y a lieu, les bénéficiaires d'une cession ou d'une subrogation des droits relatifs au contrat;
- s'il y a lieu, les juridictions concernées;
- la direction des assurances, la direction générale des impôts et tous services publics habilités à les recevoir;
- les commissaires aux comptes et les audits.

ou d'un tiers ou de la collectivité et à condition qu'elle ne porte pas atteinte aux intérêts légitimes de la personne concernée» (71). En outre, la loi allemande autorise la libre circulation de données « neutres » : « nom, titre académique, date de naissance, profession et secteur d'activités, adresse, numéro de téléphone » (§ 24, § 2 BDSG).

La législation allemande laisse au judiciaire le soin de trancher la pertinence de la transmission de certaines données et d'apprécier les intérêts en présence. Ainsi, la communication des informations recueillies auprès d'un réassureur est, selon la doctrine (72), conforme à la loi et le fiché ne peut s'y opposer; ainsi l'établissement d'une centrale de mauvais payeurs ou de mauvais risques et son alimentation par les compagnies sont légitimes (73).

27. Le projet belge contient peu de dispositions relatives à la communication des données et la notion de tiers elle-même est mal définie. On note cependant que la déclaration doit préciser « les rapprochements, les interconnexions ou toute autre forme de mise en relation des données, ainsi que les conditions auxquelles celles-ci pourront éventuellement être cédées à des tiers » (art. 26), que le registre reprend les catégories de personnes admises à obtenir les données, les conditions de communications et d'utilisation des données communiquées à ces personnes (art. 27) et que l'article 28 permet au Roi, par arrêté royal délibéré en Conseil des Ministres, de réglementer après avis de la Commission de contrôle, les rapprochements, interconnexions ou toute autre forme de mise en relation de données. Les flux transfrontières peuvent en outre être soumis à autorisation préalable selon l'article 29 du projet.

Enfin, si le projet contient une disposition relative aux données « neutres » (74), les termes du projet la rendent peu utile pour les compagnies d'assurances (75).

(71) Cf. le texte de la norme française.

(72) § 24 (1) du BDSG. Comp. § 18 de la loi autrichienne. Pour un commentaire de la disposition allemande et de nombreuses applications au monde de l'assurance, S. Simitis, in BDSG-Komm., op. cit., 713 et s. Ainsi la transmission des mauvais risques « Schlechtsrisikendata » à une centrale professionnelle est autorisée.

(73) S. Simitis, BDSG, op. cit., § 24, 24.

(74) S. Simitis, BDSG, op. cit., § 23, 57.

(75) L'article 16, § 2, b) exclut du champ d'application du chapitre II (mais non du chapitre III relatif au contrôle de la commission consultative de la vie privée): « les traitements automatisés contenant exclusivement des données à caractère personnel qui font l'objet d'une publicité en vertu d'une disposition légale ou réglementaire ou dont la personne à laquelle elles se rapportent assure ou fait assurer la publicité ». On notera l'imprécision du critère: qu'est-ce qu'une donnée faisant l'objet d'une publicité légale ou réglementaire? Ainsi une donnée judiciaire n'est-elle pas publique? Quant à la donnée publique du fait de l'assuré, quelle signification lui donner? Un numéro de téléphone l'est certes. Quid des petites annonces signées dans les journaux?

L'ensemble de ces prescrits et la peur d'une réglementation auront certainement pour effet de limiter ou du moins de rendre plus difficiles les transferts de données sur support magnétique entre courtiers et sociétés d'assurances (directement ou via leur association professionnelle) et ce, au détriment des besoins du secteur. On regrettera qu'en cette matière, le projet belge n'ait pas adopté l'approche sectorielle développée dans d'autres pays. Ainsi, à l'instar du projet français, on pourrait songer à l'adoption de normes simplifiées par secteurs d'activités, normes justifiées par la finalité propre de l'activité de ces secteurs.

F. Le contrôle des fichiers

28. Toutes les législations prévoient la désignation d'une institution spécifique du contrôle des fichiers.

Le projet belge prévoit la création d'une commission consultative de la protection de la vie privée, nommée par l'exécutif (76) et « dont le Roi règle la composition et le fonctionnement par arrêté délibéré en Conseil des Ministres ». Un arrêté royal du 20 août 1984 (77) règle cette composition et ce fonctionnement. Dans un premier temps la compétence de la commission projetée sera limitée au contrôle, d'une part, du Registre National des personnes physiques organisé par la loi du 8 août 1983 (78) et d'autre part, de la banque de données relatives aux membres du personnel du secteur public instituée par l'arrêté royal n° 141 du 30 décembre 1982 (79). Cette compétence sera étendue lors de l'adoption du projet actuellement en discussion.

La composition (80) de cette commission dans l'arrêté royal est la suivante:

(76) Le mot « exclusivement » fait tomber sous le coup de l'ensemble du projet tout traitement qui contient d'autres données que celles reprises à l'article 16, § 2, b. Or tout fichier d'assurance contiendra au moins une donnée d'identification de l'assuré, ne serait-ce que le n° de police.

(77) Arrêté royal réglant la composition et le fonctionnement de la Commission consultative de la protection de la vie privée, Mb. 26.4.1984, 5487. Sur cette Commission, cf. J. Berleur, Pouillet, A. propos de la création de deux banques de données, Droit de l'informatique, n° 2, pp. 21 et s.

(78) La loi a été publiée au Moniteur du 21 avril 1984 (p. 5247) en même temps que les arrêtés d'application, celui du 3 avril relatif à la composition du numéro d'identification des personnes inscrites au Registre national des personnes physiques, celui du 3 avril relatif à l'accès de certaines autorités publiques au Registre national des personnes physiques.

(79) Suivi par deux arrêtés royaux, du 21 avril 1984 (Mb. 26.4.1984, 5480) et du 20 avril 1984 (Mb. 26.4.1984, 5489).

(80) Sur l'importance de ces prescrits relatifs au statut, à la composition et à la mission de la commission, nos réflexions in J. Berleur, Y. Pouillet, Informatique et Vie privée, J.T., 1978, 109 et s.

- 4 membres nommés sur proposition du Ministre de la Justice dont un magistrat, un fonctionnaire du Ministère, un avocat et un membre du corps professoral de l'Université;

- 3 membres nommés sur proposition du Ministre de la fonction publique dont un fonctionnaire, un membre du corps professoral et une personne n'appartenant pas à la fonction publique choisie pour ses compétences;

- un membre, nommé sur proposition du Ministre des Affaires économiques.

La composition de la commission nous paraît orientée vers le contrôle des fichiers de l'administration.

29. La mission de cette commission (80) est importante:

1°) La commission « donne soit d'initiative, soit sur demande du Gouvernement, des chambres, des procureurs généraux ou des cours et tribunaux des avis sur toute question relative à l'application de la présente loi, eu égard notamment à l'évolution des techniques ».

En outre, elle remet d'office suivant le projet des avis préalables en plusieurs matières importantes pour les assureurs: dérogations relatives à l'utilisation de données pénales; formes simplifiées de déclarations préalables et d'inscription au registre public; réglementation des rapprochements, interconnexions et flux transfrontières.

2°) La commission procède à des investigations et des contrôles et peut requérir le concours d'experts. Avec l'autorisation du juge d'instruction, elle peut procéder à des vérifications sur place.

3°) La commission dénonce au procureur du Roi les infractions dont elle a eu connaissance. A cet égard, on notera que l'actuel projet n'a pas voulu donner à la commission, une compétence de décision. Le projet Vanderpoorten faisait de la commission à la fois un contrôleur et un censeur, ainsi, elle pouvait réglementer d'office l'utilisation d'un traitement ou en interdire l'exploitation. Ce cumul des compétences de contrôle et de décision nous apparaît dangereux et la solution de l'actuel projet a notre préférence.

(81) Quant à un aperçu relatif à la mission et au travail de la commission française (CNIL), après cinq ans d'activité, lire:

- F. Chamoux, J.P. Chamoux, H. Delahaie, La loi « Informatique et libertés, face aux entreprises », Computerrecht, 1984, n° 1, pp. 3 et s.

- N. Lenoir, H. Maisl, la CNIL et le contrôle de l'administration, Informatique et Droit, mai 1984, n° 1, pp. 3 et s.

4°) La commission remet aux chambres un rapport annuel sur l'application de la loi et les avis rendus. L'expérience étrangère, notamment française, témoigne de l'intérêt de ce rapport public.

30. L'expérience étrangère montre la nécessité pour une telle commission d'être largement ouverte à la concertation avec le milieu professionnel. Ainsi, la norme française n° 16 déjà signalée n'a pu être édictée que par la concertation avec le milieu professionnel, de même l'actuel contrôle réalisé par la CNIL sur les questionnaires écrits remis par les entreprises à leurs clients s'appuie, en ce qui concerne du moins le secteur des assurances, sur le contrôle préalable réalisé par ce qui en France correspond à notre office de contrôle des Assurances.

Aux Etats-Unis, la NAIC Model Act prévoit que c'est le « State Insurance Commissioner », c'est-à-dire l'organisation chargée du contrôle des assurances, qui exerce, elle-même et non un organisme central et global, les prérogatives de contrôle de l'application du Model Act (§§ 14-15).

Il peut procéder à l'audition de l'entreprise suspectée de violer les prescrits du Model Act, il peut requérir la production de tout document et s'il estime que la compagnie d'assurance exerce des pratiques en violation du texte, il peut ordonner la cessation de telles pratiques voire imposer une amende (§§ 17, 18A).

L'entreprise peut obtenir une révision judiciaire de cet ordre mais au cas où elle ne l'obtiendrait pas et persisterait dans la pratique incriminée, la commission fédérale de contrôle des assurances peut suspendre ou révoquer sa licence (§ 18B). Ainsi, plus le contrôle sera organisé à l'intérieur du secteur et adapté à ce dernier, plus les entreprises admettront-elles des sanctions efficaces et lourdes.

Conclusion

31. Il ne pouvait être question d'aborder et de résoudre toutes les questions soulevées par l'informatisation des entreprises d'assurances et le respect de nos libertés. Les réflexions ci-dessus permettent cependant d'affirmer quelques principes qui, à notre avis, devraient permettre de réaliser le juste équilibre souhaité par l'auteur du projet belge entre les intérêts légitimes des parties en présence. Le fiché d'une part, l'entreprise d'assurance d'autre part. La question de l'informatique et des libertés indi-

viduelles doit se résoudre par la conciliation et la définition de deux droits à reconnaître pleinement :

1. Le droit à l'information de l'entreprise d'assurance
2. Le droit à l'information du fiché.

A propos de ces deux droits, il nous paraît important de préciser :

1°) Le droit à l'information de l'entreprise d'assurance doit être consacré en tant que tel. Il tire son fondement et sa limite du but légitime poursuivi par le traitement. « C'est seulement lorsqu'on connaît cet objectif et non en raisonnant dans l'abstrait sur l'information elle-même que l'on peut tracer la limite de tolérance acceptable pour l'intéressé ». Certains objecteront l'imprécision du critère de pertinence. La critique m'apparaît peu fondée. Le critère de « pertinence » est en effet plus souple et plus respectueux d'une appréciation judiciaire évolutive que le critère a priori, réglementaire, tiré de la nature soi-disant dangereuse en soi, « des données », critère qui par opposition est peu soucieux de la réalité vivante de la relation entre l'entreprise d'assurance et son client.

A cet égard, on regrettera la longue liste de données « interdites » édictée par le projet belge, la multiplication des déclarations et procédures administratives, à charge des entreprises; on insistera par contre, sur la responsabilité des entreprises d'assurances à l'égard de la sécurité de leurs fichiers (nomination d'un gestionnaire, règles déontologiques, normes de sécurité); on affirmera la nécessité d'une réflexion en concertation avec le milieu professionnel sur la définition des besoins du secteur proprement dit et de chaque entreprise, en particulier.

2° Le droit à l'information du fiché définit comme le droit de la personne fichée de participer à la formation de l'image que les personnes qui l'entourent se font de lui est le juste corollaire du droit à l'information du collecteur. C'est le droit pour chacun de connaître « pourquoi et comment » tel est fiché, c'est le droit de connaître les circuits d'information, enfin, c'est le droit de contester les « vérités sorties de l'ordinateur ».

Pour le secteur des assurances, la reconnaissance de ces droits non point contradictoires mais complémentaires est importante. Le rapport NCC cité en introduction de cette étude concluait en effet comme suit son analyse de la pratique des compagnies d'assurances induite par les réglementations européennes de protection des données.

« L'expérience des entreprises d'assurances dans les pays où une réglementation des données est en vigueur témoigne du fait que leur activité a été peu modifiée par ces réglementations... Mieux, le fait de ces réglementations procure certains avantages aux assureurs : le public tire de la loi la conviction que les règles de sécurité et de protection des données sont respectées ».

Ainsi, la réglementation relative à la protection des données a accru la confiance des assurés dans leurs compagnies d'assurances et a amené la direction de ces dernières à mieux évaluer et prendre en considération les techniques indispensables de sécurités et de protection des données. Assureurs et assurés ont donc tout à gagner à voir adopter une bonne législation sur la protection des données, affirmant et conciliant un juste équilibre entre leurs libertés respectives.

ANNEXE N° 1

NTIA REPORT 82-98

PRIVACY PROTECTION LAW IN THE UNITED STATES

Extraits

C. Comprehensive Statutes: Insurance Information and Privacy Protection Model Act

In 1979, the National Association of Insurance Commissioners (NAIC) approved a model privacy law, the Insurance Information and Privacy Protection Model Act. 1) The purpose of the model law is to establish standards for the collection, use and disclosure by insurance companies 2) of information gathered in connection with insurance transactions. Since its issuance, ten States have enacted the NAIC Model Law, 3) either as approved or in modified form.

In addition, at least two States have enacted privacy laws relating to insurance information. A Maryland statute requires that medical files compiled by insurance companies be made available to subject of the file. Information provided by a physician may be withheld for five years unless disclosure is authorized by the physician. Md. Ann. Code art. 48A, §§ 490C, 490E. Pur-

suant to a New York statute, insurance companies that are members of a medical information exchange center or that otherwise transmit medical information to any other similar facility used by two or more insurance companies to determine an applicant's insurability must abide by certain restriction in transmitting any medical information requested from an applicant. No medical insurance exchange facility may release any medical information it may have on a person to anyone unless it has been given explicit written permission by the applicant. N.Y. Inst. Law §68-a.

1. Collection Limitation

An insurance company must give notice to all applicants or policy holders of the nature and scope of personal information that may be collected about individuals in connection with an application for insurance, a policy renewal, a policy reinstatement or a change in insurance benefits. §4(A). Such notice must be provided prior to collection of information from third parties and must include the following information: (1) whether personal information may be collected from third parties; (2) the types of personal information that may be collected and the types of sources and investigative techniques that may be used to collect such information; (3) the types of parties to whom and the circumstances under which personal information may be disclosed without prior authorization; (4) the types of personal information that may be disclosed; and (5) that a right of access, correction and amendment exists with respect to the personal information collected. §4(B).

An insurance company must specify those items of information to be collected from an individual which are desired solely for marketing, research or other purposes not directly related to the insurance transaction. §5. Any form or statement provided by an insurance company for signature by an individual authorizing disclosure of information about the individual in connection with an insurance relationship must be written in plain language and must specify (1) the types of persons authorized to disclose information about the individual, (2) the nature of the information authorized to be disclosed, (3) the types of persons to whom the individual has authorized the information to be disclosed, (4) the purposes for which the information is collected, and (5) the length of time such authorizations shall remain valid. §6.

Insurance companies may prepare or request an investigative consumer report about an individual only if the individual is infor-

med that he or she may ask to be interviewed in connection with the preparation of the report and that upon request he or she is entitled to receive a copy of the report if no personal interview is conducted. §7(A). Insurance companies also are prohibited from seeking information concerning any previous adverse underwriting decision regarding an individual, or any previous insurance coverage obtained by an individual through a residual market mechanism, unless such inquiry also requests the reasons for any previous adverse underwriting decision or the reasons why insurance coverage was previously obtained through a residual market mechanism. §11.

As a general rule, insurance companies and their agents are prohibited from obtaining information in connection with an insurance transaction by way of «pretext interviews» where the interviewer misrepresents who he or she is, who he or she is representing, or the purpose of the interview. §§2(V), 3. Such interviews are authorized only if the interviewee does not have a privileged relationship with the subject of the interview, and if the insurance company has reasonable grounds to suspect fraud, misrepresentation, or nondisclosure. §3.

2. Data Quality

As is more fully described below in subpart 7, individuals must be given an opportunity to see and copy information maintained by the insurance company relating to the individual, and to dispute the accuracy of such information. §§8-9.

In addition, the Model Act imposes limitations on the use by insurance companies of certain information in rendering adverse underwriting decisions. First, they may not rely on previous adverse insurance decisions, although such information may provide the basis for further investigation by the company. Second, insurance companies may not base adverse decisions on personal information received from an insurance-support organization whose primary source of information is insurance companies, although, again, such information may provide the basis for further investigation which may itself result in an adverse decision. §12.

Finally, as discussed above in subpart 1, insurance companies may not seek information relating to a prior adverse underwriting decision unless the reasons for such an adverse decision are also requested. §11.

3. Purpose Specification

A number of provisions set out above in subpart 1, applicable to the Collection Limitation Principle, are also applicable to the Purpose Specification Principle, including sections 4, 5, and 6, relating to notification by an insurance company of an intention to collect information about an individual and the uses to be made of such information. Section 13, more fully described below in subpart 4, sets out limitations and conditions relating to disclosure of information about an individual by an insurance company.

4. Use Limitation

Section 13 of the NAIC Model Act sets out conditions and limitations pursuant to which an insurance company may disclose information about an individual. Disclosure may be made in the following circumstances:

- (a) with the written authorization of the individual;
- (b) to enable a person to perform a business function on behalf of an insurance company;
- (c) to an insurance company, if the information disclosed is reasonably necessary to detect or prevent fraud or to perform a function in connection with an insurance transaction involving the individual;
- (d) to a medical institution or professional for the purpose of verifying coverage, informing the individual of a medical problem, or conducting an audit;
- (e) to an insurance regulatory authority;
- (f) to a law enforcement or other government authority to protect the interests of the insurance company or to report illegal activities;
- (g) if otherwise permitted or required by law;
- (h) in response to a facially valid administrative or judicial order, including a search warrant or subpoena;
- (i) for the purpose of conducting scientific research, provided that the information is protected and is destroyed when no longer needed;
- (j) to a party to a sale or merger involving the insurance company;
- (k) for use in connection with the marketing of a product or service, if the individual has not objected;
- (l) to an affiliate in connection with an audit or the marketing of a product or service;

(m) by a consumer reporting agency (subject to the Fair Credit Reporting Act);

(n) to a group policyholder for the purpose of reporting claims experience or conducting an audit;

(o) to a medical peer review organization for peer review purposes;

(p) to a governmental authority for the purpose of determining eligibility for health benefits; or

(q) to a certificateholder or policyholder, concerning the status of an insurance transaction.

In addition, as described above in subpart 2, section 12 of the Act imposes limitations on the use of previous adverse underwriting decisions and second-hand information supplied by insurance-support organizations.

5. Openness

Under the Act, if adverse action is taken by an insurance company, notification to the individual of such action must include a statement of specific reasons for the action or a disclosure of the applicant's right to a written statement of reasons upon request. § 10 (A) (1). The individual has 90 days in which to request the insurance company to provide the specific reasons for the adverse decision if such information was not provided initially, the information that supports the decision, and the names and addresses of the institutional sources that provided such information. The Act does not require an insurance company to release privileged information if it suspects fraud or misrepresentation in connection with a claim. An insurance company may elect to release specific items of health care information or the identity of medical professionals to the individual or to a medical professional designated by the individual. § 10(B).

Finally, the individual also must be advised of his or her rights regarding access to and correction of records maintained by an insurance company as well as his or her rights under section 10(B) when adverse action is taken by an insurance company. § 10(A)(2).

6. Individual Participation

If an individual submits a written request to an insurance company for non-privileged recorded personal information about the individual that reasonably describes the information requested, the company must notify the individual within 30 days of the

nature and substance of such information. The company must also permit the individual to see and copy the information and disclose to the individual the identity, if recorded, of those persons to whom the insurance company has disclosed such personal information within two years prior to such request or, if the identity is not recorded, the names of those insurance companies or other persons to whom such information is normally disclosed. In addition, the company must provide the individual with a summary of the procedures by which he or she may request correction, amendment or deletion of recorded personal information. §8(A). Any personal information provided shall identify institutional sources of the information. §8(B). Medical-record information may be supplied either directly to the individual or to a licensed medical professional designated by the individual, whichever the insurance company prefers. §8(C). Except for personal information provided to an individual relating to an adverse insurance decision, an insurance company may charge a reasonable fee to cover the costs incurred in providing information to individuals. §8(D).

Within thirty business days of receiving a written request from any individual to correct, amend or delete any recorded personal information about the individual within its possession, an insurance company must either make the requested modification, or notify the individual of its refusal to do so and the reasons for such refusal, as well as the individual's right to have a supplementary statement inserted in the records. §9(A). If the insurance company corrects, amends or deletes recorded personal information, it must so notify the individual in writing. The correction, amendment or fact of deletion also must be provided to (1) any person specifically designated by the individual who may have received such information within the preceding two years; (2) any insurance-support organization whose primary source of personal information is insurance companies if the support organization has systematically received such recorded personal information from the insurance company within the preceding seven years; and (3) any insurance-support organization that furnished the personal information that has been corrected, amended or deleted. §9(B).

If an individual disagrees with an insurance company's refusal to correct, amend or delete recorded personal information, the individual must be allowed to file with the insurance company a statement setting forth his or her view of the correct, relevant or fair information, and a statement of the reasons why the

individual disagrees with the insurance company's refusal to correct, amend or delete the information. §9(C). Any subsequent disclosure by the company must identify the matter in dispute and include the individual's statement. §9(D).

As noted above in subpart 1, an individual has a right to request a personal interview when an insurance company proposes to prepare an investigative consumer report on the individual. §7. Pursuant to section 10(B), as outlined above in subpart 6, if adverse action is taken by an insurance company, the individual against whom such action is taken has the right to request the reason for such decision, the personal information that supports those reasons, and the names and addresses of institutional sources of such information.

7. Accountability

The State insurance commissioner is granted general authority to enforce the provisions of the Model Act. The commissioner may conduct investigations of insurance companies and hold hearing relating to possible violations of the Act. The commissioner has the authority to subpoena witnesses to appear at a hearing, and to require the production of books, correspondence, records, and other documents. §§14-15.

If, after a hearing, the commissioner determines that the insurance company charged has engaged in conduct or practices in violation of the Act, he or she shall issue an order requiring the company to cease and desist from such conduct or practices, and also may impose a monetary penalty for knowing violations. §§17,18(A). Any person subject to an order of the insurance commissioner may obtain judicial review of such order. §19. Any person who violates a cease-and-desist order of the commissioner may be subject to a monetary penalty or suspension or revocation of such person's license. §18(B).

Under section 20, any insurance company that violates section 13 will be liable for actual damages sustained by the subject of the disclosure. Violations of sections 8, 9 and 10 are subject to equitable relief. Court costs and reasonable attorney's fees may be awarded to the prevailing party. The individual remedies set out in section 20 are exclusive.

Finally, any person who knowingly and willfully obtains information on a person from an insurance company under false pretenses is subject to fine and/or imprisonment. §22.

ANNEXE N° 2

DELIBERATION N° 81-04 DU 20 JANVIER 1981

concernant les traitements automatisés d'informations nominatives relatifs à la passation, la gestion et l'exécution des contrats mis en œuvre par les organismes d'assurances, de capitalisation, de réassurances et d'assistance et par leurs intermédiaires.

(Journal officiel du 5 février 1981).

Norme simplifiée n° 16.

La commission nationale de l'informatique et des libertés,

Vu les articles 6, 17 et 21 (§ 1) de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés habilitant la commission nationale de l'informatique et des libertés à édicter, en vertu de son pouvoir réglementaire, des normes simplifiées concernant certains traitements automatisés d'informations nominatives;

Vu le code des assurances;

Considérant que pour l'application de l'article 17 susvisé il faut entendre par norme simplifiée l'ensemble des conditions que doivent remplir certaines catégories les plus courantes de traitements pour être regardées comme ne comportant pas de risques d'atteinte à la vie privée et aux libertés et comme pouvant dès lors faire l'objet d'une déclaration simplifiée;

Considérant que certains traitements automatisés portant sur la passation, la gestion et l'exécution des contrats d'assurances de capitalisation de réassurance et d'assistance sont de ceux qui peuvent, sous certaines conditions, relever de l'article 17 susmentionné,

Décide:

Article 1^{er}.

Les dispositions de la présente décision concernent les traitements automatisés d'informations nominatives relatifs à la passation, la gestion et l'exécution des contrats mis en œuvre par les organismes d'assurances, de capitalisation, de réassurance et d'assistance et par leurs intermédiaires.

Pour pouvoir faire l'objet de la procédure de déclaration simplifiée, ces traitements doivent:

- ne porter que sur des données objectives aisément contrôlables par les intéressés grâce à l'exercice du droit individuel d'accès;

- n'appliquer à ces données que des logiciels dont les résultats puissent être facilement contrôlés;

- ne pas donner lieu à des cessions, locations, interconnexions ou échanges autres que ceux nécessaires à l'accomplissement des fonctions énoncées à l'article 2 ci-dessous;

- comporter des dispositions propres à assurer la sécurité des traitements et des informations et la garantie des secrets protégés par la loi;

- satisfaire en outre aux conditions énoncées aux articles 2 à 7 ci-dessous.

Article 2.

Finalité du traitement

Le traitement ne doit pas avoir d'autres fonctions que:

a) Pour la passation et la gestion des contrats:

- l'étude des besoins spécifiques de chaque demandeur afin de proposer des contrats adaptés à ses risques;

- l'examen et le contrôle du risque;

- la tarification, l'émission des polices et des documents comptables, l'encaissement des primes ou cotisations, leur répartition éventuelle entre les coassureurs, le commissionnement des intermédiaires, la surveillance des risques et les autres opérations techniques nécessaires;

b) Pour l'exécution des contrats:

- les opérations techniques nécessaires, notamment la détermination et le paiement des indemnités et prestations et, s'il y a lieu pour l'apériteur, leur collecte auprès des coassureurs, l'exécution des dispositions prévues au contrat et l'exercice des recours;

c) L'élaboration des statistiques;

d) L'établissement de sélections, parmi les clients de l'organisme, pour réaliser des actions de prospection et de promotion liées exclusivement aux activités propres à l'organisme;

e) L'exécution des dispositions légales, réglementaires et administratives en vigueur.

Article 3.

Catégories d'informations traitées

Dès lors que les dispositions de l'article 27 de la loi n° 78-17 du 6 janvier 1978 ont été respectées lors du recueil des informa-

tions traitées, celles-ci doivent relever seulement des catégories suivantes, dans le respect de la finalité de chaque type de garantie :

Pour l'ensemble des garanties :

a) Identité : nom, prénoms, sexe, adresse, numéro de téléphone, date et lieu de naissance, nationalité ;

b) Situation militaire : dans la mesure où elle conduit à la suspension de certaines garanties ou à la suspension du paiement de certaines primes ou cotisations durant le service militaire ;

c) Situation économique et financière : caractéristiques professionnelles, revenus annuels, frais généraux, identité bancaire ou postale ;

d) Informations nécessaires à l'application du contrat : par exemple, numéro client, du contrat, du dossier sinistre, mode de paiement primes ou cotisations et accessoires, commissions, taxes, créances en cours, références de l'apporteur, des coassureurs et des réassureurs du contrat, nature du sinistre, indemnités, capitaux, rentes, valeurs assurées et garanties souscrites, antécédents du risque et assurances cumulatives ;

e) Informations relatives à la détermination ou à l'évaluation des préjudices.

Pour la garanties :

f) D'assurances des véhicules terrestres à moteur : dates, caractéristiques, validité du permis de conduire et, le cas échéant, lieu de travail et déplacements professionnels, éléments entraînant une déchéance de garantie ;

g) D'assurances de dommages : renseignements sur les biens assurables ;

h) D'assurances immobilières : caractéristiques et situation du logement ou du local, conditions d'occupation ;

i) D'assurances de personnes et de responsabilité civile :

- santé (sous réserve du respect par les personnes concernées des dispositions prévues à l'article 378 du code pénal, éléments nécessaires à la passation, à la gestion et à l'exécution des contrats) ;
- situation de famille (situation et régime matrimonial, descendants, ascendants et personnes à charge) ;
- formation (niveau et nature des études en cours) ;
- loisirs (activités sportives et de plein air, sport, chasse, plaisance).

Article 4.

Durée de conservation

d La durée de conservation des informations nécessaires aux traitements automatisés d'informations nominatives définies aux articles 1^{er}, 2 et 3 ne doit pas être supérieure à celles qui résultent de la réglementation en vigueur, et notamment des articles 2262 du code civil et R. 341-4 du code des assurances. Les informations collectées autres que celles nécessaires à établir la preuve qu'un contrat n'a pas été souscrit, ne peuvent être conservées lorsqu'une proposition ou un contrat n'a pas été signé.

Article 5.

Destinataires des informations

Peuvent seuls, dans les limites de leurs attributions respectives, être destinataires des informations afférentes à chaque type de garantie :

- les personnels chargés de la passation, la gestion et l'exécution des contrats
- l'apporteur du contrat (agents, courtiers...) et son personnel ;
- les souscripteurs, les assurés et les bénéficiaires des contrats ;
- s'il y a lieu, l'organisme d'assurance des responsables de l'accident ou offrant des prestations complémentaires ;
- s'il y a lieu, les coassureurs et réassureurs ainsi que les organismes professionnels chargés de gérer le contrat ou de prévenir et de combattre la fraude ;
- s'il y a lieu, les avocats, experts, médecins et notaires ;
- les caisses de sécurité sociale lorsque les régimes sociaux interviennent dans le règlement des sinistres ou lorsque les organismes d'assurances offrent des garanties complémentaires à celles des régimes sociaux ;
- s'il y a lieu, le responsable, les victimes de l'accident et leurs mandataires ;
- s'il y a lieu, les bénéficiaires d'une cession ou d'une subrogation des droits relatifs au contrat ;
- s'il y a lieu, les juridictions concernées ;
- la direction des assurances, la direction, générale des impôts et tous services publics habilités à les recevoir ;
- les commissaires aux comptes et les audits.

Article 6.

Appréciation du risque

Seules les informations de nature à préciser les risques encourus par l'assuré au regard des intérêts professionnels légitimes de l'assureur pourront être utilisées pour établir cette appréciation. En aucun cas le traitement ne portera sur des informations relatives à la vie privée de l'intéressé. Aucune décision refusant un contrat d'assurances, de capitalisation, de réassurances ou d'assistance à une personne ne pourra avoir pour seul fondement un traitement automatisé d'informations nominatives.

Article 7.

Dispositions complémentaires

Les traitements dont les finalités sont celles définies à l'article ci-dessus, qui comportent l'enregistrement d'informations n'appartenant pas aux catégories énumérées à l'article 3 ou aboutissant à la transmission d'informations à des destinataires autres que ceux définis à l'article 5 doivent faire l'objet de demandes d'avis ou de déclarations complémentaires selon qu'ils relèvent des articles 15, 16 ou 48.

Le président,
J. THYRAUD.
